



April 12, 2021

By electronic delivery via www.federalreserve.gov

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: Docket ID No. R-1736; Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (RIN 7100-1736)

Ladies and Gentlemen:

This letter is submitted by Visa Inc., on behalf of itself and its affiliates ("Visa") in response to the federal banking agencies' proposed rule on computer-security incident notification requirements for banking organizations and their bank service providers ("Proposed Rule"). Visa appreciates the opportunity to provide comments on the Proposed Rule, as well as the coordination efforts undertaken by the Office of the Comptroller of the Currency ("OCC"); the Board of Governors of the Federal Reserve System ("Board"); and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the "Agencies"). Visa applauds the Agencies for proposing a uniform approach for computer security incident response within the banking sector, and for encouraging further transparency among regulated entities and the Agencies.

Visa plays a pivotal role in advancing payment products and technologies worldwide to benefit its more than 15,500 financial institution clients (including 9,000 financial institution clients in the U.S.) and the millions of merchants that accept Visa-branded payment cards serving consumers in the U.S. and globally. Visa's global payments network provides a number of payment processing services to banking organizations of all sizes, not only via our core VisaNet processing network but via products and services that enhance security and fraud prevention controls, cardholder benefits, and loyalty programs, to name a few. Therefore, this comment letter focuses on the Proposed Rule from the perspective of a "bank service provider".

In sum, we urge the Agencies to consider modifying the Proposed Rule to accommodate the following recommendations:

- 1) Include an option for bank service providers that serve a substantial number of financial institutions and support critical activities ("significant service providers") to notify Agencies directly of a "notification incident"; and

- 2) Harmonize the definitions of “computer-security incident” and “notification incident” so that all organizations may operate under a uniform definition.

Alternatively, we recommend narrowing the definition of “computer-security incident” to ensure the standard for notifications considers actual harm only and that such notifications only go to banking organizations directly impacted by the incident when a bank service provider has made a determination that an incident will or is reasonably likely to materially impact the services provided to the banking organizations.

Lastly, we recommend creation of a web portal for submission of notifications to encourage uniformity in process and formatting. We discuss each of these points in turn below.

- 1. The final rule should include an option for bank service providers to notify agencies directly.**

Visa strongly encourages the Agencies to modify the Proposed Rule to include an option for “significant” bank service providers to notify Agencies directly of the occurrence of a “notification incident.” Especially for a large multinational organization like Visa, which services a substantial number of clients across a number of products and services, and which is already regulated as a “significant service provider” by the Federal Financial Institutions Examination Council (FFIEC”) and subject to ongoing oversight and examination, the ability to notify the Agencies directly would streamline the notification process and ensure that regulators receive information in a timely manner. In general, “significant service providers” provide services to a substantial number of financial institutions to support “critical activities”, in particular, significant bank functions such as payments, clearing and settlement; significant shared services such as information technology or other activities that could have significant impacts on customers or on bank operations. An event that rises to the level of a “notification incident” involving a significant service provider is much more likely to affect the viability of the operations of a [large number of] banking organization[s], result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector.” This approach would also enable these service providers to operate under their existing incident response processes where clients are notified in accordance with contractual commitments and optimally allocate resources necessary to resolve and mitigate the incident, rather than expend critical resources to satisfy prescriptive notice obligations and processes that are likely to be challenging to meet during crisis management, including requirements to notify at least two individuals at affected banking organizations.

We note that the comments in the Proposed Rule state that an obligation to notify clients is not expected to greatly impact organizations’ existing processes. While it is true that organizations have existing processes under which clients are notified of incidents in accordance with contractual commitments, incident triage is always highly fact-specific, where even incidents that are ultimately ruled minor may absorb hundreds of work hours. Therefore, we believe that the Agencies may have significantly underestimated the

amount of time and resources expended, and level of automation available, on incident management. The ability to streamline this process by allowing significant bank service providers to notify the Agencies directly, as Visa already does today, helps such providers dedicate more time to appropriately assessing the incident at hand rather than spending additional hours potentially over-notifying their clients. Direct notification to Agencies in turn does not absolve bank service providers from notifying their clients, but rather ensures service providers are able to send more meaningful notifications in parallel, focusing on those clients that are directly impacted by the incident.

To the extent the Agencies adopt this recommendation, Visa would support having these significant bank service providers notify the Agencies within the same period of time as the banking organizations (timing of which is further discussed in item number four (4) below).

2. The Agencies should include only a single definition for a notification incident that applies to both bank service providers and banking organizations.

We understand that the Agencies included two definitions of incidents requiring notice (the first a “computer-security incident” and the second a “notification incident”) out of concern that a bank service provider may not be able to make an adequate determination on whether an incident could “materially disrupt, degrade, or impair” the banking organizations’ services. However, due to existing requirements such as U.S. state breach notification laws, the General Data Protection Regulation (“GDPR”) and PSD2 in the EU, and the New York Department of Financial Services’ (“NY DFS”) Cybersecurity Rule, organizations are already accustomed to reviewing incidents for certain notifiable triggers, and thus are already highly skilled at making such determinations based on a single uniform definition. If both bank service providers and banking organizations are able to rely on a single definition in order to assess whether an incident is notifiable, the resulting uniformity in how incidents are assessed increases the likelihood of better coordination between the bank service provider and its banking clients, and in turn, the Agencies. Additionally, bank service providers are already well positioned to make a determination on the materiality of an incident, as assessing the severity of the impact to both the bank service provider and its banking clients is already a critical component of any bank service provider’s incident response process.

Regardless of whether the Agencies modify the Proposed Rule to allow significant service providers to notify Agencies directly in the case of a notification incident as discussed above, Visa supports a uniform definition of “notification incident,” appropriately modified to accommodate both bank organizations and bank service providers. Moreover, we strongly encourage the Agencies to modify the definition of “notification incident” with language that more strongly emphasizes a scenario where there has been a determination that actual harm has occurred or is reasonably likely to occur. Thus, we propose modifying the beginning of the definition as follows: ‘Notification incident’ is a computer-security incident *where* a banking organization *determines* in good faith that *actual harm has occurred which will or is reasonably likely*

to materially disrupt, degrade or impair ” By changing the word “believes” to “determines,” and by changing the word “could” to “will or is reasonably likely to,” organizations are better able to ensure that the clock that starts the notification timeline is triggered once such organizations have had adequate time to assess the severity of an incident. Otherwise, the Agencies would require organizations to notify them before such organizations have adequate facts to confirm whether there is any actual risk of harm. For example, something as simple as an employee clicking on a phishing email *could* result in materially disrupting, degrading or impairing one’s systems, but such an action in isolation, without conducting forensics or other assessments to determine the extent of any installed malware, could also do little to no harm. Likewise, the subjectivity of the word “believes” could lead to assumptions being made that as soon as one person in the organization *believes* there is a problem, the notification clock begins. However, a *determination* is made based on facts gathered after an organization has had adequate time to assess an issue, and thus we believe this approach better fits the realities of an incident response plan.

3. Assuming the Agencies preserve two different “incident” definitions and therefore different notification standards, the definition of “computer-security incident” should be narrowed.

Visa believes that a harmonized “notification incident” for both bank service providers and banking organizations is the best path forward. However, in the event the Agencies preserve two definitions, the current definition of “computer-security incident” as a trigger for a notification to clients in the Proposed Rules is overbroad and should be narrowed to prevent over-notification.

First, the inclusion of “potential harm” in part (i) of the definition, rather than focusing only on actual harm, would require bank service providers like Visa to radically modify its incident response processes in order to be able to notify clients well in advance of doing an adequate assessment of whether there is any actual risk associated with the incident in question. This would lead to the likelihood that bank service providers would be flooding their clients’ inboxes with notifications, many of which would provide little to no meaningful information. In fact, too many notifications to clients run the risk of giving clients “notification fatigue” and thus potentially result in banking organizations not spending adequate time assessing those notifications. It is also possible that Agencies will in turn receive a parallel flood of notifications, given that banks will understandably be concerned about the 36-hour timeframe in which to notify, and thus err on the side of over-notifying, even if an event is later confirmed not to be a “notification incident.”

Second, we recommend that part (ii) of the definition of “computer-security incident” be removed in its entirety. While we appreciate that banking clients should be made aware of any *material* violation of a security policy that *directly impacts them*, we believe a focus on notifying in the event of actual harm would achieve this objective. Adding in a general requirement to notify a banking organization any time there is a “violation or imminent threat of violation of security policies, security procedures, or acceptable use policies” would require bank service providers to decide whether to notify

a banking organization for even minor infractions, such as when an employee misdirects an email or labels a document with the wrong classification.

Third, we strongly recommend that the obligation to notify banking organizations only relate to clients that are directly affected by a computer-security incident. Not only would this help minimize the potential flood of emails and calls going to clients about incidents, but it would allow bank service providers to more quickly respond to inquiries coming from clients that are truly impacted by the issue at hand.

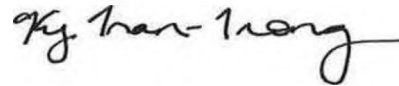
Regarding the notification requirement itself, we encourage the Agencies to remove the requirement to notify at least two contacts at each banking organization, and to ensure the requirement to notify banking organizations is only triggered once a determination has been made that actual harm has occurred, or is reasonably likely to occur. As the Agencies have acknowledged in the preamble to the Proposed Rules, bank service providers already have existing processes in place used to notify banking organizations of incidents. These processes may or may not include notifying two or more individuals at a banking organization, and often the process for notification is already agreed upon in advance via contractual terms. A requirement to overhaul our incident response processes to ensure we have identified two responsible individuals at each of our clients would take the focus away from ensuring that our existing processes for notification are meaningful and effective, regardless of the methods used and number of individuals notified. Additionally, for smaller banking organizations, it simply may not be realistic or practicable to notify more than one person, due to the need to preserve confidentiality and effectively manage the communications with such clients. Furthermore, we encourage the Agencies to replace the word “immediately” with “as soon as practicable” and to accept the same modifications we proposed to “notification incident.” Thus, a bank service provider would notify *as soon as practicable* after the bank service provider experiences a computer-security incident that it *determines* in good faith in good faith *will or is reasonably likely to materially* disrupt, degrade, or impair...”

4. The Agencies should create a web portal to allow for uniformity in process and formatting of submissions and increase the 36-hour time period to 72 hours.

While we understand from the commentary that the Agencies are open to flexibility in terms of the form and format of notifications, we strongly recommend making available a web portal that allows for uniformity in notification submissions. This helps organizations and the Agencies: 1) ensure notifications and any follow ups relating thereto are properly tracked and 2) establish standardization in the information requested and submitted. Lastly, Visa supports extending the time period for submissions to seventy-two (72) hours, including for service provider notifications, to more closely align with existing breach notification laws and provide sufficient time to develop adequate facts to determine the likelihood of actual risk of harm.

We would be happy to follow up with you on any aspects of this letter, with further supporting information or submissions. If you have any questions concerning the issues raised in this letter do not hesitate to contact me at 202-419-4109 or ktrantro@visa.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Ky Tran-Trong". The signature is fluid and cursive, with a long horizontal stroke extending from the end.

Ky Tran-Trong
Associate General Counsel, Regulatory
Visa Inc.